Notice of Allowability	Application No.	Applicant(s)	
	09/576,598	GOLOMB ET AL.	
	Examiner	Art Unit	
	Belix M. Ortiz	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *9/6/2006*.

2. ☒ The allowed claim(s) is/are *1, 3-16, 19, 21-26, 29, 31-33, 35-36*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *9/13/2006* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

C. R Jones

CHARLES RONES
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

EXAMINER'S AMENDMENT

1. The following is an Examiner's statement of reasons for the indication of allowable subject matter: The prior art of record does not disclose, make obvious, or otherwise suggest the structure of the applicant's prediction program, prediction apparatus, and prediction method together with the other limitations of the independent claims.

The dependent claims being further limiting and definite are also allowable. Any comments considered necessary by applicant must be submitted no later than the payment of the Issue Fee and, to avoid processing delays, should preferably **accompany** the Issue Fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance.

Authorization for this examiner's amendment was given in an interview with Scott C. Harris on September 13, 2006.

AMENDMENT TO THE CLAIMS:

Claims 1 and 19 have been amended. Claims 1, 3-16, 19, 21-26, 29, 31-33, and 35-36 remain pending in the application.

WHAT IS CLAIMED IS:

1. (Currently Amended) A computer implemented cryptography method, comprising:

determining information M to be encrypted; and

encrypting said information to form encrypted information using a non-trivial ci-quasigroup as a key K to create a cipher C indicative of the information M as C = M*K, where * denotes a mathematical operation, where the non-trivial ci-quasigroup has

properties that for the operation *, between any two elements in the non-trivial ci-quasigroup, a result of the operation is also in the non-trivial ci-quasigroup and for every K, as M takes on a different value, resulting values of C are each distinct, for every M, as K takes on all key values, the resulting values of C, are all distinct; and that each key K in a keyspace P has a permutation K^{-1} that decodes the encrypting, such that $K^{-1}*(M*a) = M$.

19. (Currently Amended) A computer implemented cryptography method, comprising:

determining information to be encrypted; and

encrypting said information M to form encrypted information using a Key K which is a crossed-inverse quasigroup to create a cipher C as C = M*K, where * denotes a mathematical operation, where the quasigroup has properties that for the operation *, between any two elements in the quasigroup, ~~the~~ a result of the operation is also in the quasigroup, and for every K, as M takes on different values, ~~the~~ resulting values of the cipher C, are each distinct, for every M, as K takes on all key values, the resulting values of the cipher C, are all distinct; and that each key K in a keyspace P has a permutation K^{-1} that decodes the encrypting, such that $K^{-1}*(M*a) = M$.

Reasons for Allowance

2. Claims 1, 3-16, 19, 21-26, 29, 31-33, 35-36 are allowed.

3. The following is a statement of reasons for the indication of allowable subject matter: the prior arts of records, neither anticipates nor renders obvious the following limitations as claimed:

As to claim 1, the prior art of records fail to anticipate or suggest encrypting said information to form encrypted information using a non-trivial ci-quasigroup as a key K to create a cipher C indicative of the information M as C = M*K, where * denotes a mathematical operation, where the non-trivial ci-quasigroup has properties that for the operation *, between any two elements in the non-trivial ci-quasigroup, a result of the operation is also in the non-trivial ci-quasigroup and for every K, as M takes on a different value, resulting values of C are each distinct, for every M, as K takes on all key values, the resulting values of C, are all distinct; and that each key K in a keyspace P has a permutation K^{-1} that decodes the encrypting, such that $K^{-1}*(M*a) = M$, together with the other limitations of the independent claims.

As to claim 19, the prior art of records fail to anticipate or suggest encrypting said information M to form encrypted information using a Key K which is a crossed-inverse quasigroup to create a cipher C as C = M*K, where * denotes a mathematical operation, where the quasigroup has properties that for the operation *, between any two elements in the quasigroup, ~~the~~ a result of the operation is also in the quasigroup, and for every K, as M takes on different values, ~~the~~ resulting values of the cipher C, are each distinct, for every M, as K takes on all key values, the resulting values

of the cipher C, are all distinct; and that each key K in a keyspace P has a permutation K^{-1} that decodes the encrypting, such that $K^{-1}*(M*a) = M$, together with the other limitations of the independent claims.

As to claim 29, the prior art of records fail to anticipate or suggest encrypt a message M into an encrypted message_using a key K indicative of a crossed-inverse quasigroup representation, where the quasigroup has properties that for an operation *, between any two elements in the quasigroup, a result of the operation is also in the quasigroup, and for every K, as M takes on message values, t-he resulting values of a cipher C, where $C = M*K$ are each distinct, for every M, as K takes on all key values, resulting values of the cipher C, are all distinct; and each key K in a keyspace P has a permutation K^{-1} that decodes the encrypting, such that $K^{-1}*(M*a) = M$;

send the encrypted message C; and

decrypt the encrypted_message using information indicative of the same crossed-inverse quasigroup representation, together with the other limitations of the independent claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Belix M. Ortiz whose telephone number is 571-272-4081. The examiner can normally be reached on 8-5.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

bmo

September 13, 2006

CHARLES RONES
SUPERVISORY PATENT EXAMINER